Honors Algebra 4, MATH 371 Winter 2010

Solutions 1

1. Let R be a ring. An element x of R is called *nilpotent* if there exists an integer $m \geq 0$ such that $x^m = 0$.

   (a) Show that every nilpotent element of R is either zero or a zero-divisor.

   (b) Suppose that R is commutative and let $x, y \in R$ be nilpotent and $r \in R$ arbitrary. Prove that $x + y$ and rx are nilpotent.

   (c) Now suppose that R is commutative with an identity and that $x \in R$ is nilpotent. Show that $1 + x$ is a unit and deduce that the sum of a unit and a nilpotent element is a unit.

   Solution:

   (a) Let $x \in R$ be nilpotent and let $m \geq 0$ be the minimal integer such that $x^m = 0$. If $m = 0$ then either $x = 0$ or $1 = 0$ and R is the zero ring (hence $x = 0$). If $m = 1$ then $x = 0$. If $m > 1$ and $x \neq 0$ then $0 = x^m = x \cdot x^{m-1}$ with $m - 1 > 0$ and $x^{m-1} \neq 0$ by minimality of m. Thus x is a zero-divisor.

   (b) Suppose that $x^m = 0$ and $y^n = 0$ and let N be any integer greater than $m + n$. By commutativity of R, we have the binomial theorem (same proof as usual) so in the expansion for $(x + y)^N$ every monomial has the form $a_{ij}x^i y^j$ with $i + j = N$ so either $i > m$ or $j > n$ or both. Thus, every monomial term is zero and hence $x + y$ is nilpotent. Again by commutativity, $(rx)^m = r^m x^m = 0$ so rx is nilpotent.

   (c) Suppose $x^m = 0$. Then $(1+x)(1-x+x^2-\cdots+(-1)^{m-1}x^{m-1}) = 1$ so $1+x$ is a unit. If u is any unit and x is nilpotent, $u + x = u(1 + u^{-1}x)$ is the product of two units (using that $u^{-1}x$ is nilpotent by the above) and hence a unit.

2. Let R be a commutative ring with 1 and let $f := a_0 + a_1 x + \cdots + a_n x^n$ be an element of the ring $R[x]$ (*i.e.* a polynomial in one variable over R).

   (a) Prove that f is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent.

   (b) Prove that f is nilpotent if and only if $a_0, \ldots, a_n$ are nilpotent.

   (c) Prove that f is a zero-divisor in $R[x]$ if and only if f is nonzero and there exists $r \in R$ with $r \neq 0$ satisfying $rf = 0$.

   Solution:

   (a) It follows immediately from problem 2 that a_0 a unit and $a_1, \ldots, a_n$ nilpotent implies that f is a unit. Conversely, if f is a unit then we can find $b_0, \ldots, b_m$ such that $g = b_0 + b_1 x + \cdots b_m x^m$ is the inverse of f. Observe first that $a_0 b_0$ is the constant term of $fg = 1$ and hence must equal 1; thus a_0, b_0 are units. We claim that $a_n^{r+1} b_{m-r} = 0$ for all $0 \leq r \leq m$. If $r = 0$ this is clear, as $a_n b_m$ is the leading term of $1 = fg$. For arbitrary $r > 0$ we compute that the coefficient of x^{n+m-r} in $1 = fg$ is

   $$a_n b_{m-r} + a_{n-1} b_{m-r+1} + \cdots + a_{n-r} b_m.$$

Multiplying through by a_n^r and using the induction hypothesis yields the desired conclusion. Putting $r = m$ and using that b_0 is a unit shows that a_n is nilpotent. Since f is a unit, we deduce that $f - a_n x^n$ is a unit by the previous exercise. Descending induction on n then yields the desired conclusion.

(b) If f is nilpotent, then so is a_n as f^N has leading term $a_n^N x^{nN}$. Thus $f - a_n x^n$ is nilpotent by problem 2. Now use descending induction. Conversely, if a_i is nilpotent for all i, say $a_i^{N_i} = 0$, then $f^N = 0$ for any $N > \sum N_i$ by the binomial theorem.

(c) Assume f is nonzero and let $g = b_0 + b_1 x + \cdots + b_m x^m$ be a nonzero polynomial of least degree satisfying $fg = 0$. Then $a_n b_m = 0$ and hence $a_n g = 0$ because $(a_n g)f = 0$ and $a_n g$ has degree strictly less than m. We claim that $a_{n-r} g = 0$ for $0 \leq r \leq n$. Indeed, if this holds for all $r < r_0$ then $(f - a_n x^n - \cdots - a_{n-r_0+1} x^{n-r_0+1})g = 0$ by the distributive property and the above argument then shows that $a_{n-r_0} g = 0$ as well. It follows that $b_i a_r = 0$ for $0 \leq r \leq n$ and hence that $b_i f = 0$ for all i. Since $g \neq 0$ there is some i for which $b_i \neq 0$, giving the desired conclusion. The converse is obvious.

3. Let n be a positive integer.

(a) Determine the zero-divisors of the ring $\mathbf{Z}/n\mathbf{Z}$. Prove your answer.

(b) For a prime p, let $G := \mathbf{Z}/p\mathbf{Z}$ as an abelian group (under addition of residue classes). Determine the zero divisors of the group-ring $\mathbf{Z}G$. Hint: it may help to write G multiplicatively.

Solution:

(a) The zero divisors of $\mathbf{Z}/n\mathbf{Z}$ correspond to $a, b \in \mathbf{Z}$ with the property that $a, b \notin n\mathbf{Z}$ but $ab \in n\mathbf{Z}$. By unique prime factorization, a and b must be proper divisors of n with $n|(ab)$ (just work one prime of n at a time).

(b) Let $g \in G$ be a generator, so $G = \{g^i \ : \ 0 \leq i \leq p-1\}$. Consider the map of $\mathbf{Z}$-algebras $\mathbf{Z}[X] \to \mathbf{Z}G$ sending X to $1 \cdot g$. This is obviously surjective and kills the ideal $(x^p - 1)$ so gives a surjective ring homomorphism

$$\mathbf{Z}[X]/(x^p - 1) \to \mathbf{Z}G.$$

We have a commutative diagram of rings

$$\begin{array}{ccc} \mathbf{Z}[X]/(x^p-1) & \longrightarrow & \mathbf{Q}[X]/(x^p-1) \\ \downarrow & & \downarrow \\ \mathbf{Z}G & \longrightarrow & \mathbf{Q}G \end{array}$$

with horizontal maps that are injective and vertical maps that are surjective. The right vertical map is a surjective map of $\mathbf{Q}$-vector spaces of the same finite dimension and is hence an isomorphism. It follows that the left vertical map is also an isomorphism and we must determine the zero divisors of $\mathbf{Z}[X]/(x^p - 1)$.

We have a factorization in $\mathbf{Z}[X]$

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$$

with both factors irreducible. This is clear for the first factor and for the second, call it $E(x)$ it follows from Eisenstein's criterion applied to

$$E(x+1) = ((x+1)^p - 1)/x = x^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} x^k$$

with the prime p using that $\binom{p}{k}$ is divisible by p for $1 \leq k \leq p-1$ and not divisible by p^2 for $k = p-1$. Since $\mathbf{Z}[X]$ is a UFD so irreducible implies prime, we deduce that for $f, g \in \mathbf{Z}[X]$, the product fg is in the ideal $(x^p - 1)$ if and only one of f, g is a multiple of $x^p - 1$ or one of f, g is a multiple of $(x-1)$ and the other is a multiple of $E(x)$. We conclude that the zero divisors of $\mathbf{Z}[X]/(x^p - 1)$ are

$$(x-1)\alpha \quad \alpha \notin (E(x)) \qquad \text{and} \qquad E(x)\beta \quad \beta \notin (x-1).$$

4. List all subrings of $\mathbf{Z}/60\mathbf{Z}$. Which of these have an identity?

   Solution: The subrings of $\mathbf{Z}/60\mathbf{Z}$ are in bijective correspondence with the subrings of $\mathbf{Z}$ containing $60\mathbf{Z}$, or in other words the ideals of $\mathbf{Z}$ containing $60\mathbf{Z}$. These are $d\mathbf{Z}$ for d dividing 60, i.e. $d = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

5. Prove that $x \in M_n(\mathbf{C})$ is nilpotent if and only if its only eigenvalue is zero. Show in particular that every strictly upper-triangular matrix (i.e. zeroes along and below the main diagonal) is nilpotent.

   Solution: If x is nilpotent then $x^n v = 0 = 0 \cdot v$ for all $v \in \mathbf{C}^n$ and hence every eigenvalue of x is zero. Conversely, if the eigenvalues of x are zero then the characteristic polynomial of x must be T^n as its only roots must be 0. Since every matrix is a root of its characteristic polynomial by the Cayley-Hamilton theorem, we conclude that $x^n = 0$ and x is nilpotent. The final statement follows immediately from the fact that the determinant of an upper-triangular matrix is the product of its diagonal entries.